

Appl. No. 09/599,124
Amdt. dated August 1, 2004
Reply to Office Action of June 23, 2004

REMARKS/ARGUMENTS

I. Introduction

- Claims 1-32 remain in this application.
- Claims 1 and 19 are currently amended.
- Claims 1-32 stand rejected.
 - Claims 1-8, 10-25, and 26-32 stand rejected under 35 U.S.C. § 102(e).
 - Claims 9 and 26 stand rejected under 35 U.S.C. § 103(a).
- Claims 1 and 19 stand objected to because of informalities.
- Claims 1 and 19 are the only independent claims.
- The drawings stand objected to “because part of them are handwritten.”

II. In the Drawings

The examiner had objected to the original drawings “because part of them are handwritten.” Applicant’s copy of the drawings has no handwritten text. Therefore, to satisfy the requirement to overcome this objection, applicant respectfully submits a new set of clean replacement sheets that include no substantive changes. Because no substantive changes have been made to the drawings, no annotated sheets are included. The attached three (3) sheets of drawings replace the original three (3) sheets of drawings. Because the replacement sheets of drawings have no handwritten text, withdrawal of this objection is respectfully requested.

Appl. No. 09/599,124
Amdt. dated August 1, 2004
Reply to Office Action of June 23, 2004

II. Amendments to the Claims

Claim 1:

Claim 1 has been amended to correct an informality that was objected to by the examiner and to incorporate a new limitation. The informality was corrected by amending the phrase "with a key registers" to read as "with a key register." The new limitation was added by modifying the phrase "key management functions" to read as "a plurality of key management functions, said plurality of key management functions including a plurality of unwrap operations; wherein the type of an unwrapped key produced is determined by which one of said plurality of unwrap operations is used."

Claim 19

Claim 19 has been amended to correct an informality that was objected to by the examiner and to incorporate a new limitation. The informality was corrected by amending the phrase "an data type" to read as "a data type." The new limitation was added by modifying the phrase "performing key management function on at least one key register using a key management algorithm" to read as "performing one of a plurality of key management functions on at least one key register using a key management algorithm, said plurality of key management functions including a plurality of unwrap operations; wherein the type of an unwrapped key produced is determined by which one of said plurality of unwrap operations is used."

III. Rejections under 35 U.S.C. § 102(e)

Appl. No. 09/599,124
Amdt. dated August 1, 2004
Reply to Office Action of June 23, 2004

A. Independent Claims 1 and 19

Applicant believes that Claims 1 and 19 as amended are not anticipated by Ober (U.S. Patent No. 6,307,936) because Ober requires EXPLICIT key typing information to determine the type of an embedded red key that is being unwrapped, whereas in the present invention, the type of the unwrapped key is ENTIRELY DETERMINED by the unwrapping function used.

Ober describes (see Ober, column 7, line 29) an external form for keys (e.g., the black form of red keys), in which the encrypted key blob contains within it EXPLICITLY the type of the encrypted key (e.g., referred to as KEK or DEK in Ober, and KK or DK in the present application). Ober's unwrap function inspects this explicit typing information when determining the type of the embedded red key that is being unwrapped.

In the present application, a wrapped key contains NO explicit typing information (see Application, page 17, lines 16-24). The type of the unwrapped key is ENTIRELY DETERMINED by the unwrapping function used. If the right unwrap function is used, then the resultant key will be a useful key of the type produced by that unwrap function; if the wrong unwrap function is used, then the resultant key will be a string of useless bits.

The typing information that is present in the present inventions (red) key registers is determined by the unwrap function used. It is NOT EXTRACTED from information in the wrapped key blob. In contrast, in Ober, the typing information in the key registers is determined from the typing information explicitly stated in the wrapped key blob.

Appl. No. 09/599,124
Amdt. dated August 1, 2004
Reply to Office Action of June 23, 2004

An advantage of the present invention over Ober is that implicitly typed information is both more compact and more secure. Because Claims 1 and 19 have been amended to claim this important distinction between Ober and the present invention, Applicant believes that currently amended Claims 1 and 19 are now allowable.

B. Dependent Claims 2-18

Applicant believes that amended Claim 1 is now in condition for allowance for at least the reasons stated above. Claims 2-18 ultimately depend on Claim 1 and hence contain all of the limitations of that base claim. Therefore, withdrawal of the rejections against those claims is respectfully requested.

C. Dependent Claims 20-32

Applicant believes that amended Claim 19 is now in condition for allowance for at least the reasons stated above. Claims 20-32 ultimately depend on Claim 19 and hence contain all of the limitations of that base claim. Therefore, withdrawal of the rejections against those claims is respectfully requested.

III. Conclusion

For all of the reasons advanced above, Applicant respectfully submits that the application is in condition for allowance and that action is respectfully solicited. If there are any outstanding issues that might be resolved by an interview or an Examiner's

Appl. No. 09/599,124
Amdt. dated August 1, 2004
Reply to Office Action of June 23, 2004

amendment, the Examiner is requested to call Applicants' agent at the telephone number shown below.

The Commissioner is hereby authorized to charge any additional fees which may be required for this amendment, or credit any overpayment, to Deposit Account No. 50-1450.

In the event that an extension of time is required, or may be required in addition to that requested in a petition for an extension for time, the Commissioner is requested to grant an extension a petition for that extension of time which is required to make this response timely and is hereby authorized to charge any fee for such an extension of time or credit any overpayment for an extension of time to Deposit Account No. 50-1450.

Respectfully submitted,

David G. Grossman
Registration No. 42,609

Date: December 21, 2004

Patent-Services.com
1408 Bayshire Lane
Herndon, VA 20170
(703) 338-6333